REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

The Applicant wishes to note that a change in correspondence address form has been filed concurrently herewith.

The Applicant also wishes to note the change in Attorney Docket number for this application.

In the Office Action, the Examiner has indicated that formal drawings are required. Accordingly, a set of formal drawings is submitted herewith.

The Examiner has rejected claims 1-5, and 8-9 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,502,135 to Munger. Claim 1 has been amended, and is believed to overcome this rejection.

The method recited in claim 1 has been amended to better describe the steps involved in resolving a web site address. The following summarizes the amended steps:

a) connecting a public host having a software module with a virtual private network (VPN) and having the software module route future domain name requests to a domain name server (DNS) of the VPN while the connection is active;
b) the software module monitoring domain name requests from the public host;
c) the software module intercepting the requests;
d) the software module modifying the requests and routing the requests to the DNS of the VPN;
e) the DNS resolving the requests and returning an address location to the

software module as a domain name response;

f) the software module modifying the response; and

g) the software module forwarding the address location to the public host.

Support for these amendments can be found in Figure 2, and in the description on page 5, line 15 to page 6, line 25. Therefore, the Applicant believes that no new subject matter has been added with this amendment.

Munger teaches various network protocols for secure communications, and in one embodiment describes a system for creating a virtual private network (VPN) in response to a domain name server look up function. The following summarizes this embodiment, which can be found in Munger at column 38, lines 23 to 42; column 39, lines 42 to 52; and Figures 25 and 26.

In this embodiment, Munger provides a domain name server (DNS) proxy that intercepts all DNS look up functions from a client and determines whether access to a secure site has been requested. If such a request has been made, the DNS proxy determines whether the client has security privilege to access the secure site. If the client does have the privilege, the DNS proxy transmits a request to a gatekeeper to set up a VPN between the client and the requested secure web site. Munger describes using "hopblocks", which are a way of securely transmitting IP packets to create a secure communication between the client and the requested secure site. The gatekeeper provides hopblocks to the client computer and the VPN for use while the client accesses the secure site. Thereafter, the DNS proxy returns to the client, the resolved address passed to it by the gatekeeper, preferably using a secure administrative VPN.

Claim 1 requires a software module of the public host to monitor and intercept domain name requests, then modify and route these requests to a DNS of a VPN. The DNS resolves the requests and returns an address location to the software module as a response, and the software module modifies this response and forwards the address location to the public host. As described on pages 5 and 6, this effectively "fools" the host in thinking that it is communicating with a

DNS of its internet service provider (ISP), since the public host typically may only receive address locations from the ISP DNS, which are not associated with private sites. Therefore, the software module, by intercepting and modifying the domain name requests, may allow the public host to access private web sites as well as the usual public internet traffic without re-configuring the public host or its ISP DNS in order to do so.

Munger sends domain name requests directly to a DNS proxy, which is used to monitor the requests and decide whether to send the request to the gatekeeper. More specifically, Munger sends domain name requests directly to a DNS proxy from the client wherein the DNS must be configured to detect whether a private site has been requested, and thereinafter send such a request to a gatekeeper which determines whether the client has the privilege to access the secure web site.

Munger does not teach having a software module of the public host modify domain name requests in order to "fool" the public host into permitting access to secure web sites. In fact, the public host (client) is configured to have no discretion regarding secure and non-secure websites, since both types of requests are sent directly to the DNS proxy, and then re-directed to the gatekeeper.

Moreover, Munger does not teach intercepting requests, the client intentionally sends the requests to the DNS proxy. There is nothing in Munger that suggests intercepting requests. Munger is entirely silent in that regard. In fact, there is no need for Munger to intercept the requests, since Munger explicitly requires that all requests are intentionally sent to the DNS proxy, and then to the gatekeeper. There are no steps taught in Munger wherein a client effectively "fools" itself in order to access private websites. Since the requests are purposefully sent to the DNS proxy, there is no need to modify the requests nor responses from the gatekeeper for that matter. The DNS proxy is configured to receive unmodified requests, and expects these unmodified requests so that it may determine whether the client is requesting access to a secure or non-secure website. Such a determination is used in deciding whether or not to forward the request to the gatekeeper.

Accordingly, Munger fails to teach a software module of a public host monitoring, intercepting and modifying domain name requests and re-modifying a response from a VPN.

Therefore, it is believed that Munger does not teach all of the steps recited in claim 1, particularly steps b), c), d) and f) outlined above. As such, it is believed that claim 1 clearly and patentably distinguishes over Munger, and is in condition for allowance.

The Applicant notes that claims 2 and 3 have been cancelled. The limitations of claims 2 and 3 are substantially covered by the amendments made to claim 1. Claim 4 has been amended, in order to change its dependency to claim 1, and to conform with the language used in the amended claim 1. Claims 5-11 have also been cancelled in this response.

Claims 12 to 16 have been added in this response. Support for claims 12 and 13 can be found on page 5, line 29 to page 6, line 11; support for claims 14 and 15 can be found on page 6, lines 12 to 13; and support for claim 16 can be found on page 7, lines 1 to 3. Therefore, it is believed that no new subject matter has been added.

Accordingly, claims 4, and 12-16 are either directly or indirectly dependent on claim 1, and as such, are also believed to patentably distinguish over the Munger reference.

Claim 17 has been added in this response. Claim 17 replaces cancelled claim 8, which was directed to an apparatus, and is now described as a system for resolving a web site address. Claim 17 describes a system suitable for implementing the method of claim 1, and as such similar arguments with respect to Munger apply. Claims 18 and 19 have also been added in this response, being dependent on claim 17. Therefore, claims 18 and 19 are also believed to distinguish over Munger.

Therefore, in summary, claims 1, 4, and 12 to 19 are believed to patentably distinguish over the Munger reference, and as such, are believed to be in condition for allowance.

The Examiner has also rejected claims 6 to 7, and 10 to 11 under 35 U.S.C. 103(a) as being unpatentable over Munger in view of U.S. Patent No. 6,425,003 to Herzog et al. This rejection is directed to claims which have been cancelled in this response. However, the Applicant will show that the amended claims also distinguish over this combination.

As noted above, claims 1 and 17 are believed to patentably distinguish over Munger. As such, the missing elements from Munger would at least have to be present or suggested in Herzog et al. in order for a person skilled in the art to consider the two references an obvious combination.

Herzog is directed towards a method and apparatus for forwarding DNS requests for a user that is simultaneously logged into more than one service (eg. ISP and intranet). Herzog utilizes an active service list (ASL), which contains a list of services to which a user is currently connected to or logged onto. The ASL is sorted based on the number of potential IP addresses associated with each entry in the list. When a DNS request packet is generated by the user and received by a gateway, the ASL is checked to determine how to proceed. A comparison of domain names is then performed, and if a match is found, the DNS request packet is modified so that the IP address of the DNS service associated with the match is inserted for the IP destination address of the DNS request packet. This forces the DNS request packet to be routed to the selected DNS service rather than, eg., the default DNS service selected by the user when their operating system is configured.

Herzog does not teach a software module at a public host monitoring, intercepting and modifying domain name requests in order to allow a user to be connected to a virtual private network. In fact, Herzog is entirely silent as to resolving a web site address for a public host connected with a virtual private network.

Herzog, therefore, fails to teach the missing elements of claims 1 and 17 not taught by Munger. Therefore for at least that reason, claims 1 and 17 are believed to patentably distinguish over the combination made by the Examiner.

Herzog uses an active service list to determine where a request packet is to be directed, and does not monitor, intercept and modify these packets in order to enable a client to connect to a virtual private network. Although Herzog does modify the request packets to allow the packet to be directed to an appropriate DNS service, this does not teach how a web site address can be resolved when a public host is connected to a virtual private network.

Moreover, Herzog does not teach using a software module of the client to intercept the requests. As shown in Figure 2, the request packets are sent to a gateway, which is a separate module connected to the host network used to determine where the request packets should be forwarded.

It is also apparent from Figure 2 that Herzog does not receive a response, which is then modified and sent back to the client. The system taught by Herzog only provides a one-way routing system to enable a gatekeeper to control the destination of a request.

It shall also be noted, that since Herzog et al. does not deal with resolving a website for connecting a public host to a virtual private network, it is directed towards an entirely different technology than Munger. Therefore, there exists no motivation to combine Herzog with Munger, since they perform entirely separate tasks, and achieve entirely different outcomes.

Therefore, the combination of Herzog et al. and Munger not only fails to teach all of the elements recited in claims 1 and 17; but there would be no motivation to combine the two references, since they handle IP traffic in entirely different ways, and achieve entirely different results.

Claims 4, 12-16, and 18-19 are dependent on either claims 1 or 17, and as such, are also believed to distinguish over the combination made by the Examiner.

In summary, claims 1, 4, and 12 to 19 are believed to describe patentable subject matter with respect to the references cited by the Examiner, and as such, are believed to be in condition for allowance.

The Applicant also wishes to note that the paragraphs under the heading "Summary of the Invention" have been replaced with an amended set of paragraphs to conform with amended claim 1 and new claim 17. However, no new subject matter has been added.

The Applicant respectfully requests early reconsideration and allowance of the present application.

Respectfully submitted,

John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: April 4, 2005

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164
JRO/BSL/dm

Amendments to the Drawings

The attached sheets of drawings will replace the drawings previously submitted.